AMENDMENTS TO THE SPECIFICATION

Please note that the following amendments are made by replacement, rather than strike-through and underlining, because they involve mathematical expressions that cannot be properly annotated with strike-through and underlining.

Please replace the paragraph beginning on Page 10, line 16, provided below:

The leftmost (i.e., least significant) 10 bits of B consist of all 12 bits of A except $(x_{13} \oplus k_{20})$ and $(x_{12} \oplus k_{19})$. We can infer the values of $(x_{13} \oplus k_{19})$ and $(x_{12} \oplus k_{19})$ by logically XORing bits of B together. By the properties of the XOR operator:

$$(b_{12} \oplus b_6) = (k_{20} \oplus k_{18}) \oplus (x_{13} \oplus k_{18}) = (x_{13} \oplus k_{20})$$
$$(b_{11} \oplus b_5) = (k_{19} \oplus k_{17}) \oplus (x_{12} \oplus k_{17}) = (x_{12} \oplus k_{19})$$

with the paragraph:

The leftmost (i.e., least significant) 10 bits of B consist of all 12 bits of A except $(x_{13} \oplus k_{20})$ and $(x_{12} \oplus k_{19})$. We can infer the values of $(x_{13} \oplus k_{20})$ and $(x_{12} \oplus k_{19})$ by logically XORing bits of B together. By the properties of the XOR operator:

$$(b_{12} \oplus b_6) = (k_{20} \oplus k_{18}) \oplus (x_{13} \oplus k_{18}) = (x_{13} \oplus k_{20})$$
$$(b_{11} \oplus b_5) = (k_{19} \oplus k_{17}) \oplus (x_{12} \oplus k_{17}) = (x_{12} \oplus k_{19})$$